

A photograph of a hippopotamus swimming in a body of water. The hippo's head and ears are above the surface, and its body is partially submerged. The water is dark green and slightly rippled.

# ***HIPAA***

## ***A Look Inside***

# Why HIPAA?

## The 104th Congress

Sought to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.



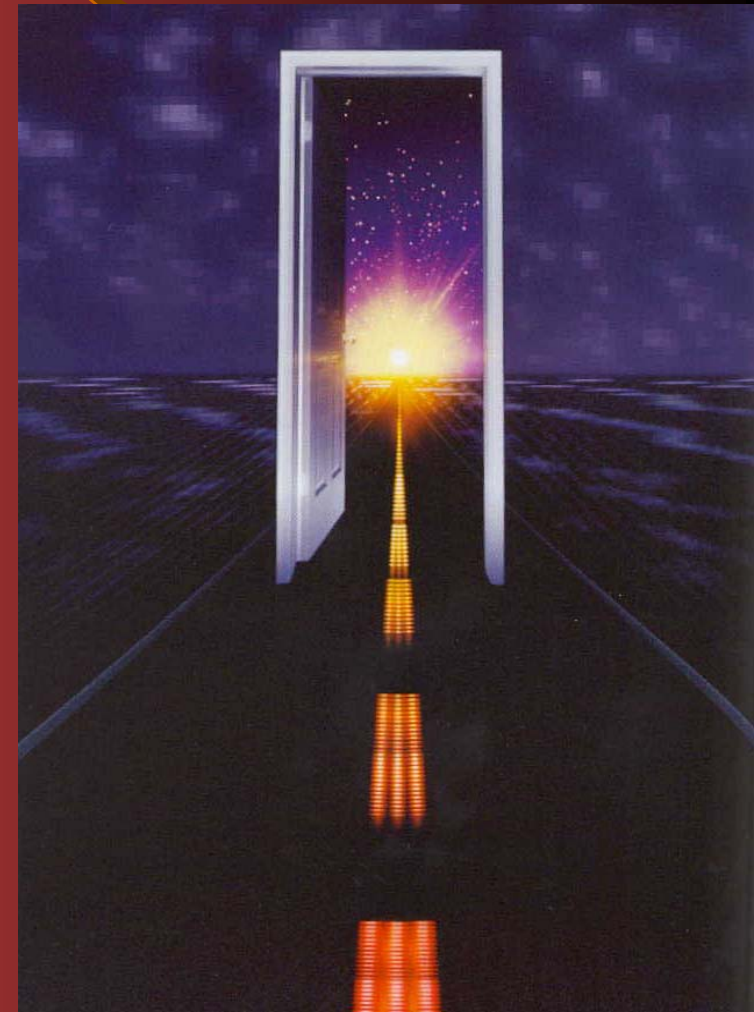
# **A National Effort to Standardize-- HIPAA!**

The Health Insurance Portability and Accountability Act of 1996, Administrative Simplification, requires payers, providers, and claims clearinghouses to establish protections, adopt standards, and meet requirements for the transmission, storage, and handling of certain health care information.

# HIPAA

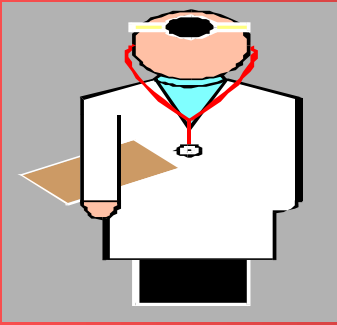
## Expected To Evolve Over Time...

- The Secretary (HHS) may adopt a modification to a standard once a year
- The Secretary may adopt a modification at any time during the first year after the standard is adopted
  - Compliance date can be as early as 180 days after modification is adopted
  - Small health plan compliance date can be extended

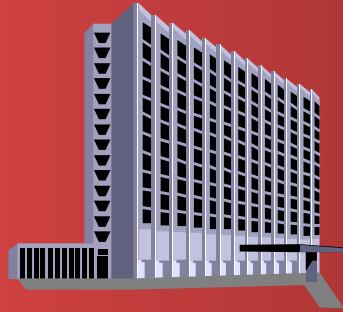


# HIPAA

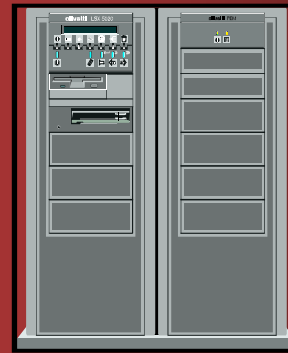
## Scalable To All Covered Entities...



**Health  
Care Providers**



**Hospitals**



**Claims  
Clearinghouses**



**Payers**

*Think "reasonable" when deciding on implementation activities*

# Does HIPAA Apply To Me?

Most medical practitioners and health care facilities that exchange protected health care information with another covered entity must comply with HIPAA

- Those excluded from HIPAA today are likely to be effected later on...
  - H.R. 3323
  - Kennedy's proposed Efficiency in Health Care Act, S. 2638
  - Private payer requirements

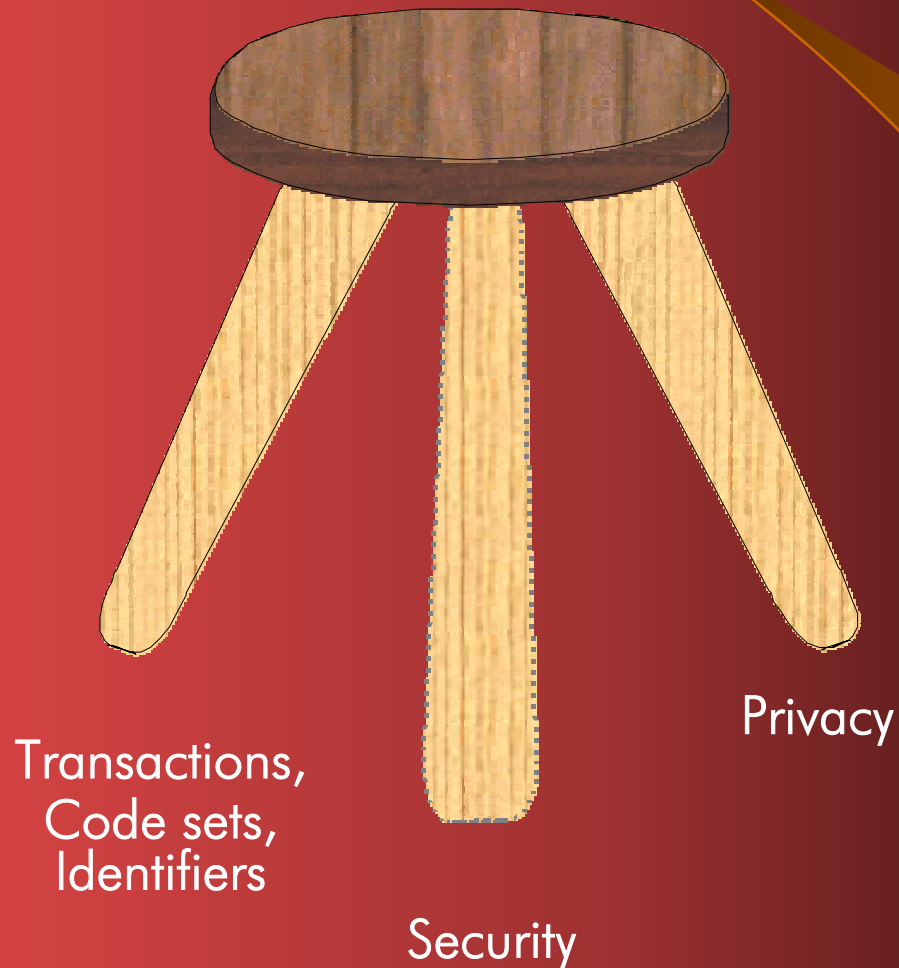
# HIPAA Pluses

- Determining real time eligibility before any services/products are rendered or supplied
- Receiving patient information before the patient arrives
- Exchanging electronic patient information with others each time an entry is made
- Having ALL costs reimbursed the same day products/services are provided

**HIPAA Makes All This Possible!**

# Administrative Simplification

## Three Components





# HIPAA

## Sound Documentation Is Essential

- Transaction Standards & Code Sets
- Privacy
- Security



Policies and Procedures

A graphic featuring a blue rectangular box with the text "Policies and Procedures" in white. To the left of the box is a vertical image of a modern building with a glass facade and a green lawn in front.

# Policies And Procedures Updates & Deletions

- Practitioners must keep policies and procedures current to comply with changes in the law, standards, and requirements
- Changes in policies and procedures are only effective from that point in time forward
- Practitioners can make policy and procedure changes at any time
- Must reviewed by all workforce during training

# HIPAA Enforcement

## “A Carrot And Not A Stick”

- Robin Frohboese, Principal Deputy & Acting Director of the Office for Civil Rights has stated that identified violations are viewed as an opportunity to educate covered entities back into compliance.
  - *“It’s critically important that covered entities understand their responsibilities and that we help them with compliance so our enforcement is minimized. If we find violations, we will seek voluntary compliance. It will only be in the most egregious situations where we are not able to get voluntary compliance that we will do other things, such as civil monetary penalties or, in the worst situations, refer to the Justice Department.”*

Source: Report on Patient Privacy, May 2002

# Accountability

- *Civil penalties* against a covered entity that fails to comply
  - \$100 per incident
  - Up to \$25,000 per person/year/standard violated
  - Enforcement by HHS Office for Civil Rights
- *Federal criminal* penalties for knowingly and improperly disclosing or obtaining protected health information
  - Up to \$250,000 and up to 10 years in prison
  - Enforcement by Department of Justice

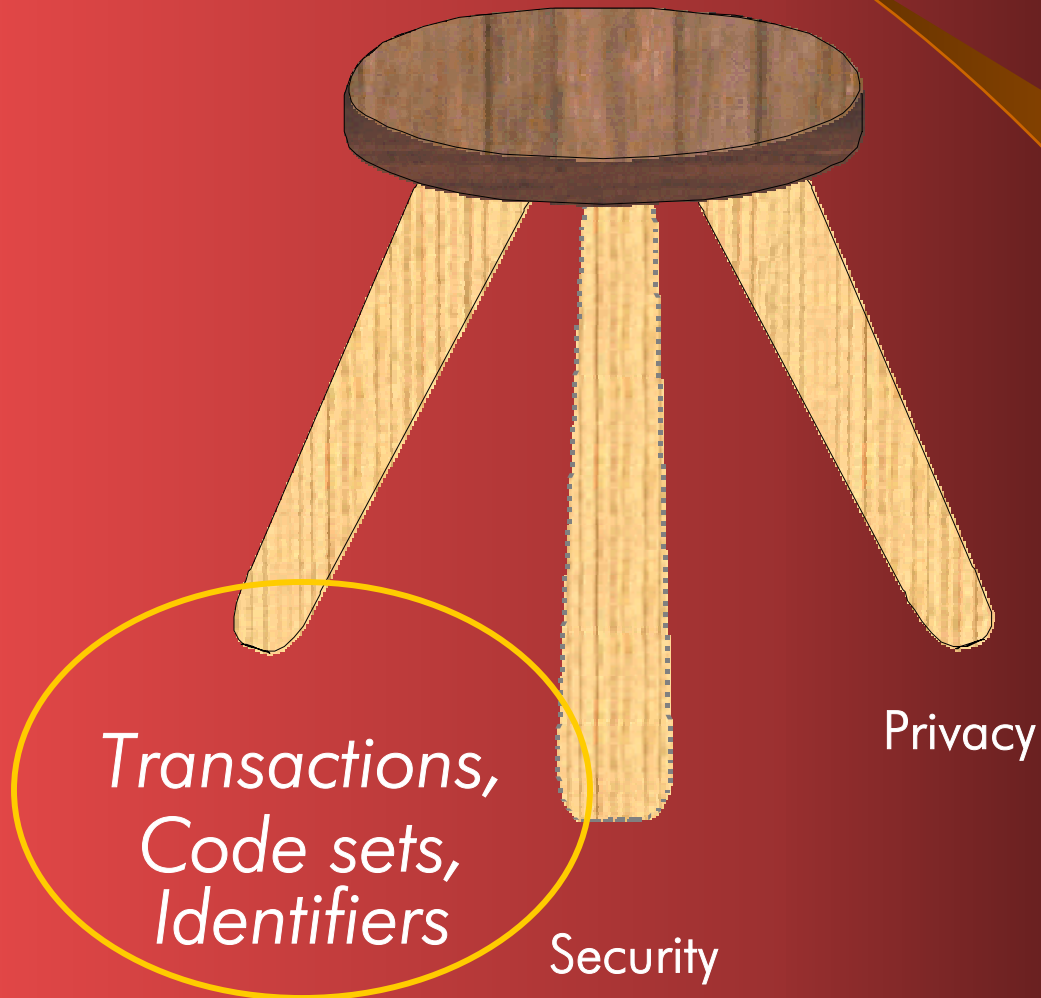


# Compliance Monitoring

- Centers for Medicare and Medicaid Services (CMS) monitors compliance on the transaction and code set standards
- The Office for Civil Rights will monitor compliance on the privacy and security regulations
- Audits can be unannounced
- Keep compliance activities in perspective

# HIPAA

## Transactions & Code Sets



# **Coordinate System Compliance Activities With Your Vendor**

- Evaluate your options for compliance (system vendor or claims clearinghouse) just in case...
- Obtain timeline for complying with X12 rules
- Self-certify or use external agency
- Talk with other users of the system

# Claims Clearinghouse – A System Vendor Option

- A claims clearinghouse can take non-compliant transactions (NSF) and convert them to the HIPAA standard
- Claims clearinghouse is likely to charge for conversion
- Requires some mapping between your system and claims clearinghouse
- Only consider as when system vendor is non-compliant



# HIPAA Transactions

## Standardize Health Information

- Payers and electronic health networks must be capable of electronically accepting:
  - Enrollment in a health plan,
  - Eligibility for a health plan,
  - Health claims (retail drug, dental, professional, and institutional)
  - Health care payment & remittance advise
  - Health plan premium payments,
  - Health claim status,
  - Referral certification, authorization, coordination of benefits (Rx: NCPDP Telecommunication Guide)

# HIPAA

## Transaction Validation Testing

- *Type 1*: EDI syntax integrity
- *Type 2*: HIPAA syntactical requirements – loops, valid segments, elements, codes
- *Type 3*: Balancing – Claim, remittance, COB, etc.
- *Type 4*: Situational requirements – Inter-segment dependencies
- *Type 5*: External Code Sets – X12, ICD-9, CPT, HCPCS

# HIPAA

## Transaction Validation Testing (Continued)

- *Type 6: Product Type, Specialty, or Line of Business – Oxygen, spinal manipulation, ambulance, anesthesia, DME, etc.*
- *Type 7: Trading Partner Specific – Medicare, Medicaid, Other payer business partner requirements (business to business testing – not HIPAA compliance testing)*

# System Vendor Programming--- Implementation & Companion Guides

- Implementation guides are required system vendor programming for type(s)/level(s) 1-6
- Companion guides are payer specific, business-to-business programming for type/level 7
- Private payers not expected to issue until early 03

# Sample X12 Coding

ST\*275\*1001~

BGN\*11\*0001\*19980429~

NM1\*PR\*2\*HEALTH CARE SERVICE

CORPORATION\*\*\*\*\*PI\*00121~

PER\*IC\*MEDICAL REVIEW DEPARTMENT~

NM1\*85\*2\*LOYOLA UNIVERSITY MEDICAL

CENTER\*\*\*\*\*FI\*364015560~

NM1\*QC\*1\*SMITH JOHN\*\*\*\*\*HN\*111223333A~

REF\*IK\*1722634842~

DTP\*472\*RD8\*19980401-19980411~

LX\*01~

STC\*R3:30005-0~

DTP\*097\*D8\*19980429~

CAT\*UL\*HL~

EFI\*09~

SE\*13\*1001~

# Transaction Testing The Value

- Validates transactions for X12 accuracy
- Tests both outbound and inbound transactions
- Directs submitter to exact X12 error(s)
- Allows for multiple submissions per transaction



# Transaction Testing Certification Vendors

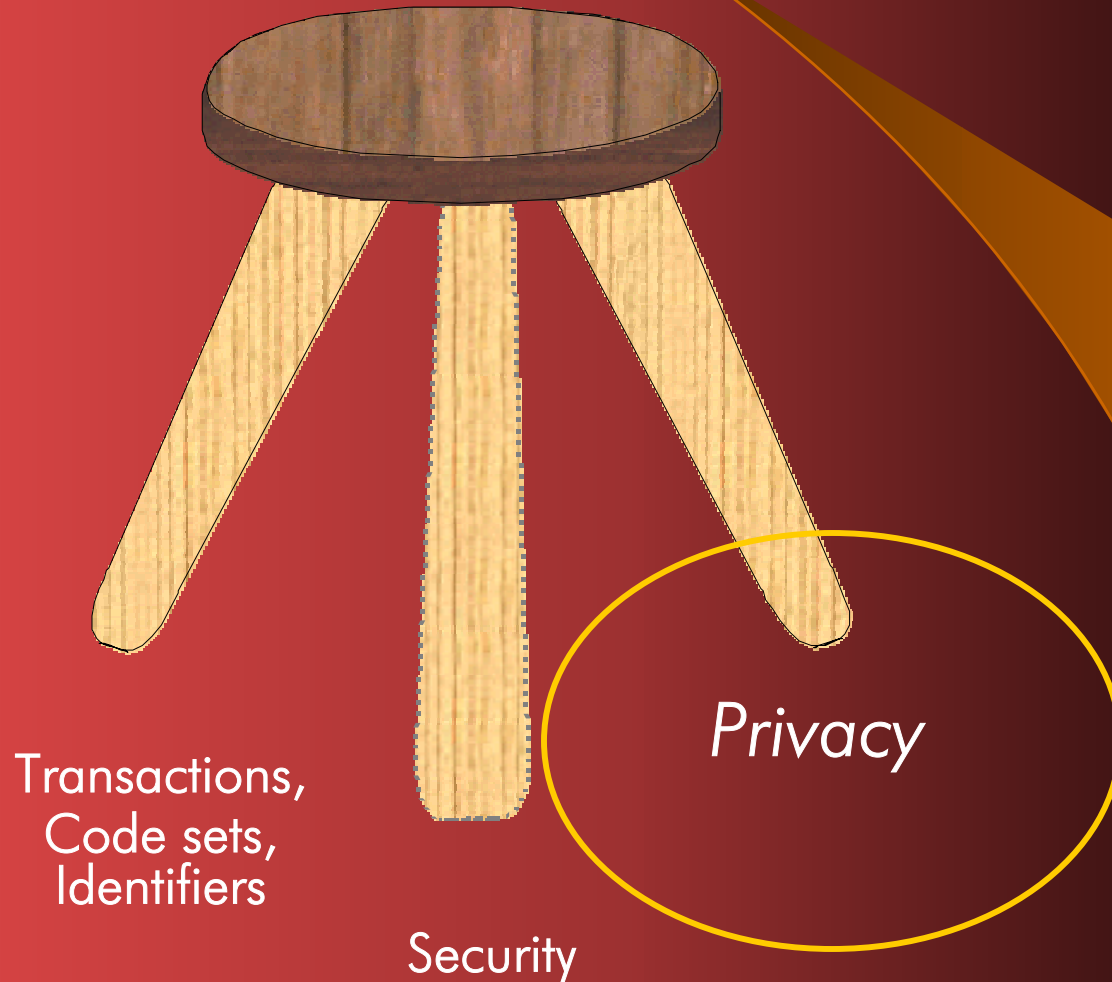
- Claredi – [www.claredi.com](http://www.claredi.com)
- EDIFECS – [www.edifecs.com](http://www.edifecs.com)
- Foresight Corporation – [www.foresight.com](http://www.foresight.com)
- GFEGUSA – [www.gfeg.com](http://www.gfeg.com)
- AppLabs, Inc. – [www.app;abs.com](http://www.app;abs.com)

# **HIPAA Transactions.... You Manage The Process**





# HIPAA Privacy



# Why Do We Need Privacy Regulations?



Mary – our car insurance is up. Seems you have a 24% chance of developing narcolepsy based on your father having diabetes.

Steven—you are to begin therapy, as your blood test indicates 25% risk of teenage depression based on your genetic profile.

Father just got a telemarketing call from a home blood sugar monitoring service. But I don't think he ever followed up on that office visit to the doctor!

# HIPAA

## Privacy Regulations

- *Protected Health Care Information (PHI) is defined as:*

Individually identifiable health care information created or received by a provider, payer, or claims clearinghouse related to health condition, provision of health care, or payment for health care

The final rule was extended in scope to include the protection of all individually health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes PHI in paper records that never have been electronically stored or transmitted

# Privacy Rule Leading Modifications Summarized

- Remove the consent requirement – strengthen requirement to notify patients about their privacy rights and practices
  - Ask patients to acknowledge receipt of privacy notice
- Health Care professionals can discuss a patient's treatment with other care providers
- Additional one-year to obtain signed Business Associate Contracts
- Marketing – Must obtain the individual's specific authorization before sending any marketing materials
- Accounting for PHI disclosures not required with an authorization

# Protected Health Information (PHI)

## The 19 Identifiers

- Name
- Address
- E-mail
- Dates
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate Number
- License Number
- Vehicle Identifiers
- Facial Photographs
- Telephone Numbers
- Device Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Geographic Units
- Any Other Unique Identifier Or Codes

# Provider Discretion

- *Did you know that...*

“A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual’s best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protect health care information.”

- Page 44 (3) Limited uses and disclosures when the individual is not present, 2<sup>nd</sup> sentence of the Final Privacy Rule – Regulation Text



# Permitted Uses & Disclosures Research

- A covered entity may use or disclose protected health care information for research, regardless of the source of funding of the research provided that approval is obtained by a:
  - Privacy Board
  - Institutional Review Board
- Limited data set allows use of PHI providing 16 identifiers are removed and a Data Usage Agreement is signed. A limited data set excludes specific, readily identifiable information

# Uses and Disclosures – Marketing and Fundraising

- Must obtain an individual's prior written authorization for marketing purposes except:
  - Face-to-face
  - Products of minimal value
  - Concerns health-related products judged beneficial
  - Communication involving a promotional gift
    - *Must take steps to allow opt out*
- May disclose to fundraising arm without authorization
  - Dates of care, limited demographic data
  - Must provide opportunity to opt out



# Minimum Necessary Concept

- When using or disclosing reasonable efforts must be made to limit PHI to that necessary to accomplish the intended purpose
- Applies to discloser and requestor
  - *Uses:*
    - Role based access
    - Need to identify types of workers, types of information, and condition of access
  - *Disclosures:*
    - Routine disclosures
    - Non-routine disclosures
- *Does not apply to disclosure to providers for treatment*

# Confidential Communications

- A covered entity must permit an individual to request, and it must accommodate reasonable requests to receive communications of PHI by provider by alternative means and location
  - Some examples: E-mail, pager, voice mail, friends/relatives home, other possibilities

# Consent - Optional

- A consent allows a provider to use or disclose protected health care information to carry out treatment, payment, & health care operations
- One time only:
  - Inform that protected health information may be used or disclosed for treatment, payment, or health care operations
  - Refer to notice of privacy practices
  - State the right to request restrictions
- May condition treatment based on consent
- May be revoked
- Provider must document & retain consent forms
- Attempts to obtain a consent must be documented

# Authorization

- Authorization is more detailed and specific than consent
  - Limited to only information to be disclosed
  - Recipient of information
  - Includes an expiration date
- Core elements of a valid authorization
  - A description of the information to be used or disclosed
  - The name or other specific identification of the person authorized to make the requested uses and disclosures
  - An expiration date or expiration event
  - A statement of the individual's right to revoke the authorization in writing
  - A statement that information used or disclosed may be subject to re-disclosure by the recipient
  - Signature of the individual and date
- Authorizations must be written in plain language

# Notice Of Privacy Practices – Things To Think About

- An individual has the right to adequate notice of the uses and disclosures of protected health care information
- The covered entity must provide a notice that is written in plain language
- Direct treatment providers to make a good faith effort to obtain a patient's written acknowledgement of the notice
- In emergency situations, the notice must be provided as soon as is reasonably practical
- Notice can be mailed

# Notice Of Privacy Practices - Elements

- Notice can be layered with summary information at the top and more detailed information at the bottom
  - *Header:* This notice described how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.  
Clarification of an individuals privacy rights
  - *A description and at least one example* of the types of uses and disclosures
  - *A description of each of the purposes* for which the covered entity is permitted or required to disclose PHI

# Notice Of Privacy Practices - Elements

(Continued)

- *A statement that uses and disclosures* follow more stringent State or Federal laws
- *A statement that other uses and disclosures* will be made only with the individuals written authorization and that the individual may revoke such authorization
- *Separate statements for certain* uses or disclosures
- *Complaint contact*
- *Contact name* for obtaining other information
- *Effective date*

# Notice Of Privacy Practices - Elements

(Continued)

- *Revision practice* and distribution process
- *Providers must provide* on the first date of service
- *Notice must be available on site* for distribution and prominently posted
- *A notice must be maintained on a covered entity's Web site* that provides customer service or benefit information



# Individual Access To PHI

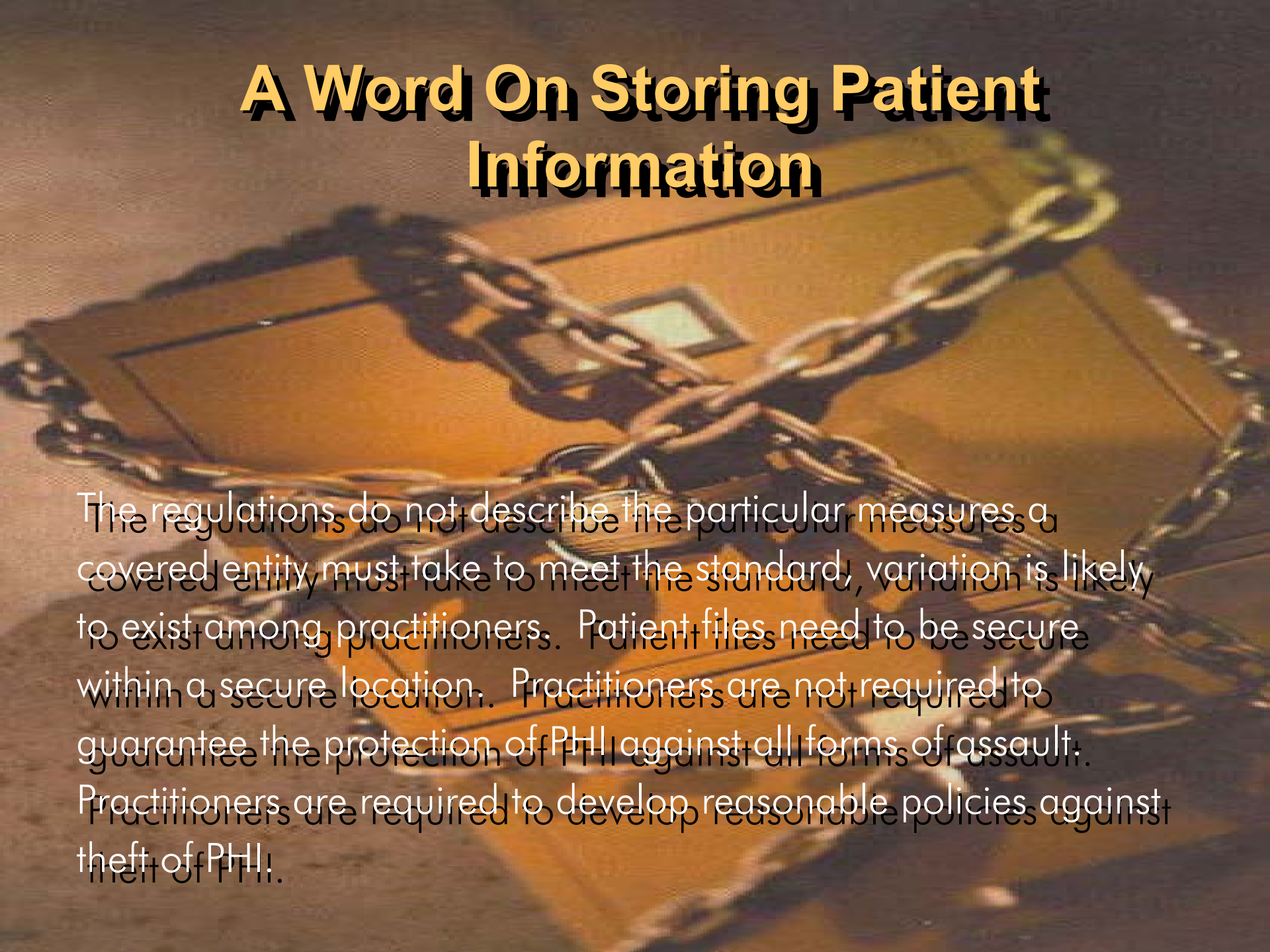
- Must permit access within 30 days of the request
  - One 30 day extension is permissible
- Ordinary access for as long as information is maintained
  - Practitioner discretion relating to psychiatric notes
  - Information compiled as part of a civil, criminal, or administrative action is exempted
- Unreviewable grounds for denial
  - Information created as a result of research – temporarily

# Individual Access To PHI

(Continued)

- Information was obtained by someone other than the health care provider under a promise of confidentiality
- Reviewable grounds for denial
  - In some circumstances a request can be reviewed by another licensed professional
  - Usually relates to professional judgment

# A Word On Storing Patient Information

The background of the slide is a close-up photograph of a metal safe. The safe is dark-colored, possibly black or dark grey, and has a prominent combination dial on its front. A heavy, silver-colored metal chain is wrapped around the handle area of the safe, further emphasizing the theme of security and protection. The lighting is somewhat dramatic, with highlights on the metal surfaces.

The regulations do not describe the particular measures a covered entity must take to meet the standard, variation is likely to exist among practitioners. Patient files need to be secure within a secure location. Practitioners are not required to guarantee the protection of PHI against all forms of assault. Practitioners are required to develop reasonable policies against theft of PHI.

# What About Sign In Sheets?

- HIPAA does not require practitioners to use sign in sheets
- Consider its purpose and value
- Look for opportunities to limit potential disclosure of PHI
- *Evaluate low cost alternatives*



# Expanded Patient Rights (NEW)

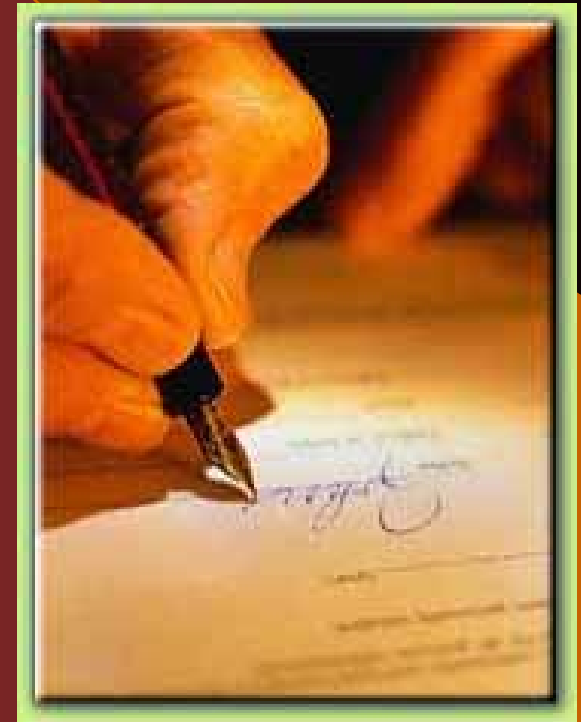
- Right to inspect and copy protected health information
- Right to amend
- All approve uses and disclosures
- Right to an accounting of disclosures
- Right to have reasonable requests for confidential communication accommodated
- Right to file a written complaint
- Right to receive written notice of information practices



# **Business Associate Contract**

## ***An Agreement Between Parties***

- Acts on behalf of a covered entity in conducting activities involving use of PHI
- Covered entities are not responsible for actions of business associates
- Monitoring is not required
- An organization can be both a covered entity and a business associate
- Due April 04

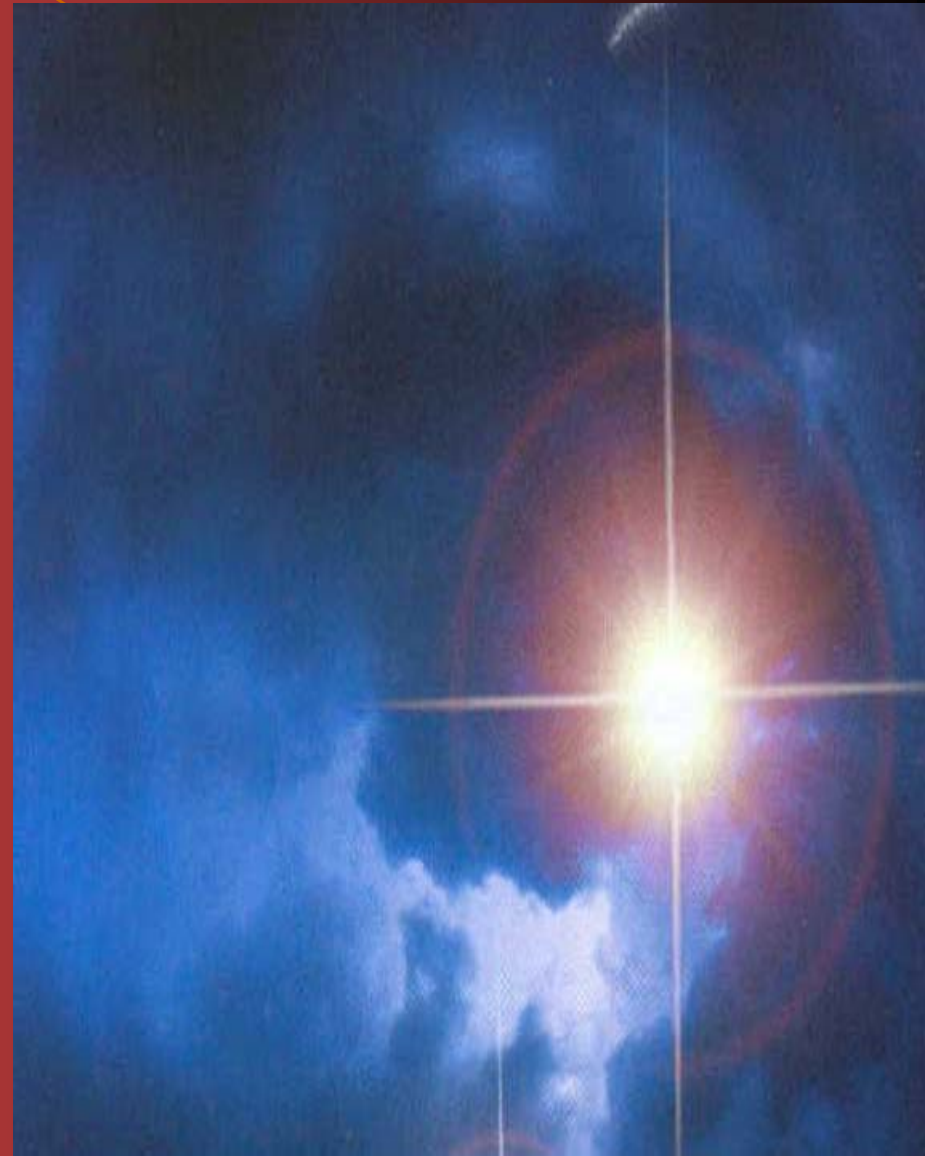




# Business Associate Contract

(Continued)

- Limit contents to information specific to PHI
- Trading partners will be reluctant to sign complex Business Associate Contracts
- Trading partners are less likely to incur legal fees on easy to read Business Associate Contracts
- Keep it simple



# HIPAA

## Business Associate Contract

### Maryland Health Care Commission

#### Sample Business Associate Contract Form:

*This form is provided without any warranty, expressed or implied, as to its legal effect and completeness. Use of this form is entirely at your own risk.*

#### THIS CONTRACT:

Is entered into on this \_\_\_\_\_ day of \_\_\_\_\_, 2001, between  
Provider/Plan/Clearinghouse and Vendor/Person(s).

#### WITNESSETH:

WHEREAS, COVERED ENTITY will make available and/or transfer to BUSINESS ASSOCIATE certain information, in conjunction with goods or services that are being provided by BUSINESS ASSOCIATE to COVERED ENTITY, that is confidential and must be afforded special treatment and protection. WHEREAS, BUSINESS ASSOCIATE will have access to and/or receive from COVERED ENTITY certain information that can be used or disclosed only in accordance with this Contract and the HHS Privacy Regulations.

#### COVERED ENTITY and BUSINESS ASSOCIATE:

Agree as follows: Limits On Use And Disclosure Established By Terms Of Contract. BUSINESS ASSOCIATE hereby agrees that it shall be prohibited from using or disclosing the information provided or made available by the covered entity for any purpose other than as expressly permitted or required by the contract.

The term of this Contract shall commence as of \_\_\_\_\_ (the Effective Date), and shall expire when all of the information provided by COVERED ENTITY to BUSINESS ASSOCIATE is destroyed or returned to the covered entity.

#### THE PARTIES:

Hereby agree that BUSINESS ASSOCIATE shall be permitted to use and/or disclose information provided or made available from the covered entity for the following stated purposes: Include a general statement describing the stated purposes that BUSINESS ASSOCIATE may use or disclose the information. These uses and disclosures must be within the scope of the BUSINESS ASSOCIATE'S representation of the covered entity.

Additional purposes for which the BUSINESS ASSOCIATE may use or disclose information:

1. BUSINESS ASSOCIATE is permitted to use information if necessary for the proper management and administration of BUSINESS ASSOCIATE or to carry out legal responsibilities of BUSINESS ASSOCIATE.
2. BUSINESS ASSOCIATE is permitted to disclose information received from COVERED ENTITY for the proper management and administration of BUSINESS ASSOCIATE or to carry out legal responsibilities of BUSINESS ASSOCIATE, provided the disclosure is required by law; or the BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, the person will use appropriate safeguards to prevent use or disclosure of the information, and the person immediately notifies the BUSINESS ASSOCIATE of any instance of which it is aware in which the confidentiality of the information has been breached.

### Maryland Health Care Commission

3. BUSINESS ASSOCIATE is also permitted to use or disclose information to provide data aggregation services, as that term is defined by 45 C.F.R. 164.501, relating to the healthcare operations of the covered entity.

4. BUSINESS ASSOCIATE will establish and maintain appropriate safeguards to prevent any use or disclosure of the information, other than as provided for by the contract.

#### REPORTS OF IMPROPER USE OR DISCLOSURE:

BUSINESS ASSOCIATE hereby agrees that it shall immediately report to the Covered Entity any discovery use or disclosure of information not provided for or allowed by the contract.

#### SUBCONTRACTORS AND AGENTS:

BUSINESS ASSOCIATE hereby agrees that anytime information is provided or made available to any subcontractors or agents, BUSINESS ASSOCIATE must enter into a subcontract with the subcontractor or agent that contains the same terms, conditions, and restrictions on the use and disclosure of information as contained in the contract. Businesses Associate must obtain the Covered Entity's approval prior to entering into such agreements

#### RIGHT OF ACCESS TO INFORMATION:

BUSINESS ASSOCIATE hereby agrees to make available and provide a right of access to information by the Individual in accordance with 45 F.R.R. 164.524, including substitution of the words Covered Entity with Business Associate where appropriate.

#### AMENDMENT AND INCORPORATION OF AMENDMENTS:

BUSINESS ASSOCIATE agrees to make Information available for amendment and to incorporate any amendments to information in accordance with 45 C.F.R. 164.526, including substitution of the words covered entity with BUSINESS ASSOCIATE where appropriate.

#### PROVIDE ACCOUNTING:

BUSINESS ASSOCIATE agrees to make information available as required to provide an accounting of disclosures in accordance with 45 C.F.R. 164.528, including substitution of the words covered entity with BUSINESS ASSOCIATE where appropriate.

#### ACCESS TO BOOKS AND RECORDS:

BUSINESS ASSOCIATE hereby agrees to make its internal practices, books, and records relating to the use or disclosure of information received from, or created or received by BUSINESS ASSOCIATE on behalf of the covered entity, available to the Secretary or the Secretary's designee for purposes of determining compliance with the privacy regulations.

#### RETURN OR DESTRUCTION OF INFORMATION:

At termination of the contract, BUSINESS ASSOCIATE hereby agrees to return or destroy all information received from, or created or received by BUSINESS ASSOCIATE on behalf of the covered entity. BUSINESS ASSOCIATE agrees not to retain any copies of the information after termination of the contract. If return or destruction of the information is not feasible, BUSINESS ASSOCIATE agrees to extend the protections of the contract for as long as necessary to protect the information and to limit any further use or disclosure. If BUSINESS ASSOCIATE elects to destroy the information, it shall certify to the covered entity that the information has been destroyed.



# HIPAA

## Business Associate Contract

(Continued)

### Maryland Health Care Commission

**MITIGATION PROCEDURES:**

BUSINESS ASSOCIATE agrees to have procedures in place for mitigating, to the maximum extent practicable, any deleterious effect from the use or disclosure of information in a manner contrary to the contract or the privacy regulations.

**SANCTION PROCEDURES:**

BUSINESS ASSOCIATE agrees and understands that it must develop and implement a system of sanctions for any employee, subcontractor or agent who violates this agreement or the privacy regulations.

**PROPERTY RIGHTS:**

The information shall be and remain the property of the covered entity. BUSINESS ASSOCIATE agrees that it acquires no title or rights to the information, including any de-identified information, as a result of the contract.

**CONTRACT TERMINATION:**

BUSINESS ASSOCIATE agrees that the covered entity has the right to immediately terminate the contract and seek relief under the Disputes Article if the covered entity determines that BUSINESS ASSOCIATE has violated a material term of the contract.

**GROUND FOR BREACH:**

Any non-compliance by BUSINESS ASSOCIATE with the contract or the privacy regulations will automatically be considered to be a grounds for breach, if BUSINESS ASSOCIATE knew and failed to immediately take reasonable steps to cure the non-compliance.

**DISPUTES:**

Any controversy or claim arising out of or relating to the contract will be finally settled by compulsory arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association, except for injunctive relief as described below.

**INJUNCTIVE RELIEF:**

Notwithstanding any rights or remedies provided for in the contract, the covered entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of information by BUSINESS ASSOCIATE or any agent, contractor or third party that received information from BUSINESS ASSOCIATE.

**MISCELLANEOUS:**

The contract shall be binding on the parties and their successors, but neither party may assign this agreement without the prior written consent of the other, which consent shall not be unreasonably withheld.

**NOTICES:**

Whenever under the contract one party is required to give notice to the other, such notice shall be deemed given if mailed by first class United States mail, postage prepaid:

Company Name: \_\_\_\_\_ Address: \_\_\_\_\_

Contact Person: \_\_\_\_\_ Title: \_\_\_\_\_

### Maryland Health Care Commission

**COVERED ENTITY:**

[Name/Address] either party may at any time change its address for notification purposes by mailing a notice stating the change and setting forth the new address.

**BUSINESS ASSOCIATE:**

[Name/Address] either party may at any time change its address for notification purposes by mailing a notice stating the change and setting forth the new address.

**GOOD FAITH:**

The parties agree to exercise good faith in the performance of the contract.

**ATTORNEY'S FEES:**

Except as otherwise specified in the contract, if any legal action or other proceeding is brought for the enforcement of the contract, or because of an alleged dispute, breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of the contract, each party shall bear their own legal expenses and the other cost incurred in that action or proceeding.

**ENTIRE AGREEMENT:**

The contract consists of this document, and constitutes the entire agreement between the parties. There are no understandings or agreements relating to this agreement which are not fully expressed in the contract and no change, waiver or discharge of obligations arising under the contract shall be valid unless in writing and executed by the party against whom such change, waiver or discharge is sought to be enforced.

**IN WITNESS WHEREOF:**

BUSINESS ASSOCIATE and COVERED ENTITY have caused this Contract to be signed and delivered by their duly authorized representatives, as of the date set forth above.

BUSINESS ASSOCIATE COVERED ENTITY

By: \_\_\_\_\_

By: \_\_\_\_\_

Print Name: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

# Administrative Requirements

- Implementation allows for flexibility and scalability
  - Response can be geared to your environment
- Covered entities are required to:
  - Designate a privacy official
  - Develop policies and procedures
  - Notices of practices
  - Provide privacy training to its workforce
  - Develop a system of sanctions for employees who violate the entity's policies
  - Meet documentation requirements

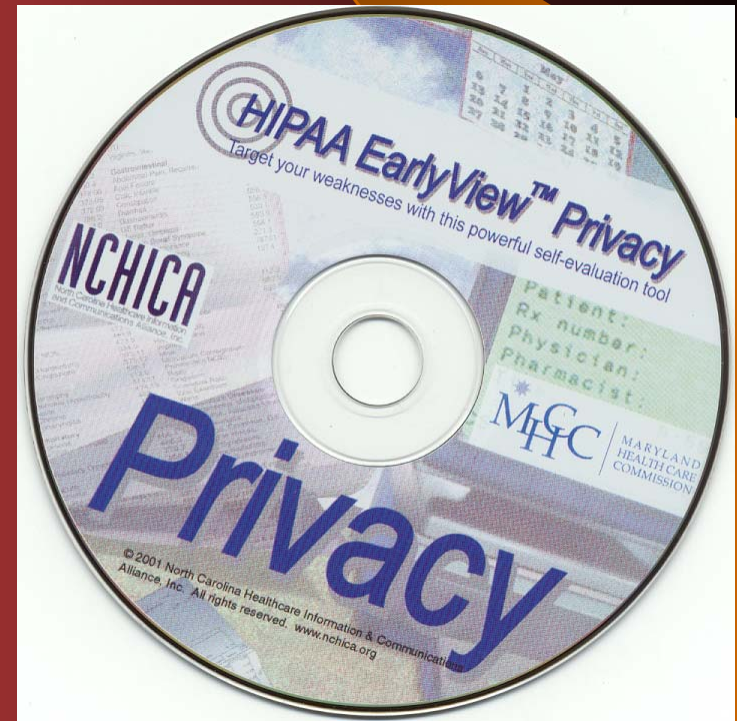
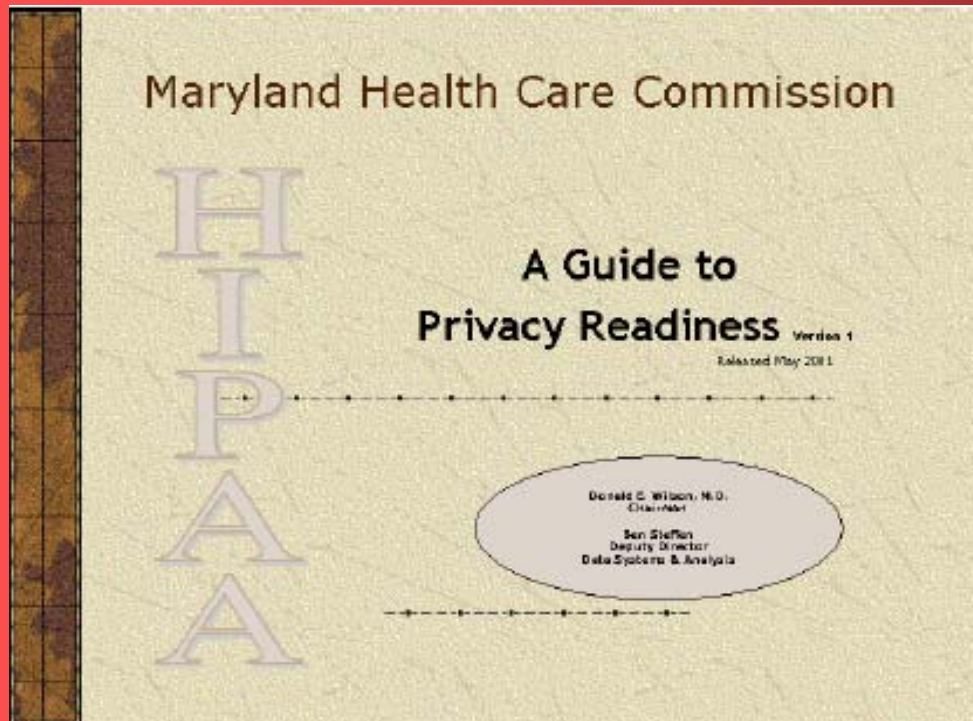
# Administrative Requirements ( Continued)

- A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law
- When a covered entity changes a privacy practice that is stated in the notice, it may make the change effective for PHI that was created or received prior to the date of the notice providing the notice reserves the right to make such change in its privacy practices
- A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented

# HIPAA Assistance For Providers

- An easy to use gap assessment tool for providers:

*Both are available at the MHCC Web-site*



# Privacy Readiness Assessment Guide

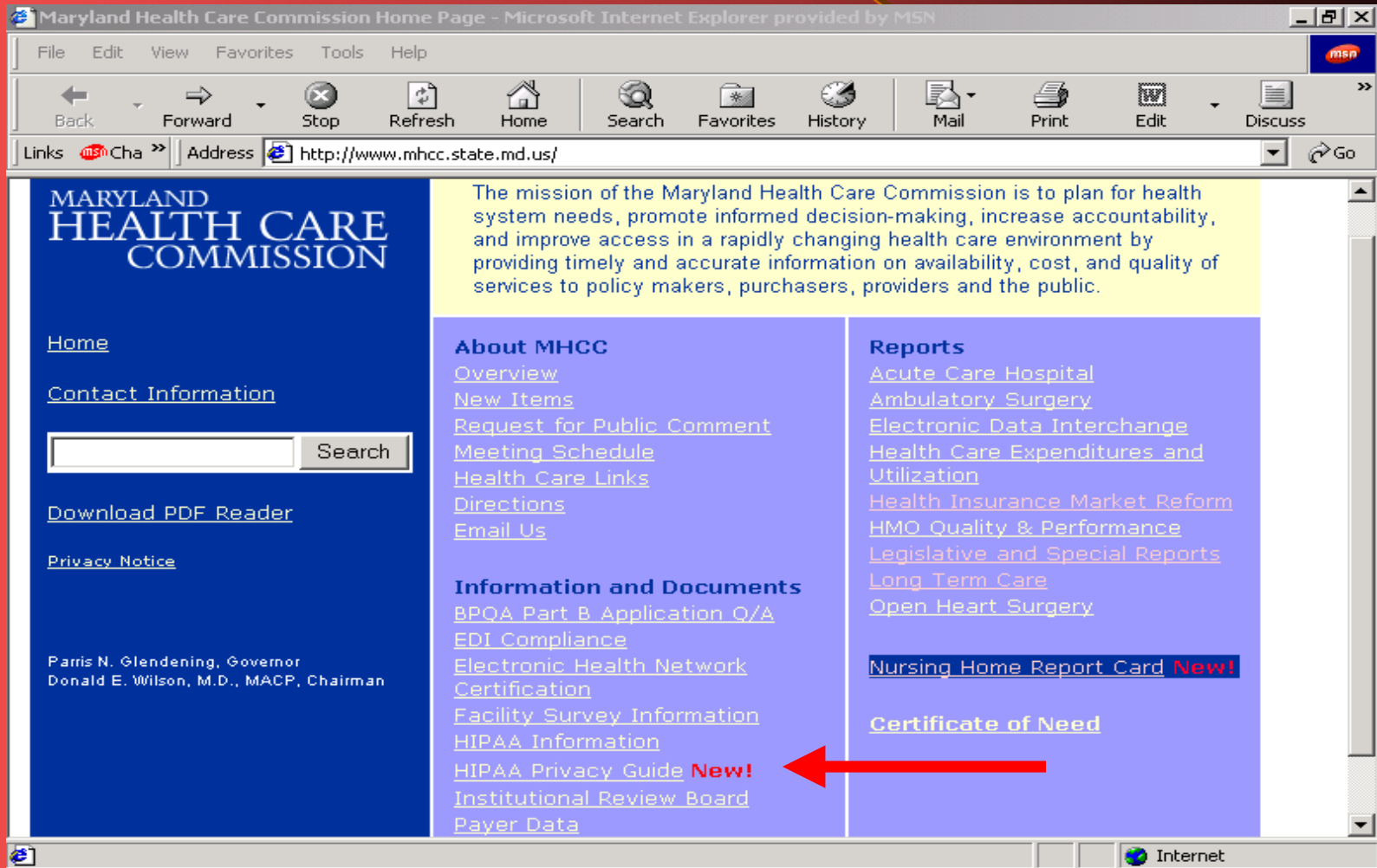
*“A Real Help To Providers”*

- The EDI/HIPAA Workgroup decided on eight sections:
  - Introduction
  - Maryland Law on the Confidentiality of Medical Records
  - HIPAA Definitions
  - Assessment Guide and Work Plan
  - Business Associate Contract (illustrative document)
  - Chain of Trust Partner Agreement (illustrative document)
  - Notice of Privacy Practices (illustrative document)
  - Computer and Information Usage Agreement (illustrative document)

## IV. ASSESSMENT GUIDE AND WORK PLAN

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p><b>Uses &amp; Disclosures of PHI (PHI)</b></p> <p>§164.502(a)</p> <p>Operational</p>	<p><i>Privacy rules require consent for disclosure of PHI for treatment, payment and health care operations, and authorization for all other purposes for which written permission is required.</i></p> <p><b>? Have you made a distinction between consent and authorization documents and added the appropriate language for use and disclosure of PHI?</b></p> <p><i>Clarification:</i> Consents are required for providers and optional for health plans. Consent may be a condition for receiving treatment. Authorizations are required for all other disclosures and require detail.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➡	<ul style="list-style-type: none"> <li>Update existing consents, authorizations to bill, and other forms used for the release of medical records. Add language stating that written consent is required for the use and disclosure of PHI for treatment, payment and health care operations.</li> </ul> <p>➡ <input type="radio"/> Not applicable   <input type="radio"/> Needs developing</p>
<p><b>Uses &amp; Disclosures for which an authorization is required</b></p> <p>§164.508</p> <p>Operational</p>	<p><i>Core Elements of an Authorization are: A specific description of the information to be disclosed, the name or other specific identification of the person(s) making the request, expiration date, a statement of the individual's right to revoke, statement that information used or disclosed may be subject to re-disclosure, signature and date, if signed by a representative a description of the authority.</i></p> <p><b>? Does your authorization document contain all the required elements for disclosure of PHI?</b></p> <p><i>Clarification:</i> Authorizations are required to be more specific than consents regarding disclosure of PHI.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➡	<ul style="list-style-type: none"> <li>Specify intended use of PHI in authorization forms. Indicate in the document that authorizations go beyond consent for release of information for purposes other than payment, treatment, and health care operations</li> <li>Where applicable, indicate in the authorization form examples of intended uses PHI and what circumstances an authorization is required, for example disclosure of psychotherapy notes.</li> </ul> <p>➡ <input type="radio"/> Not applicable   <input type="radio"/> Needs developing</p>

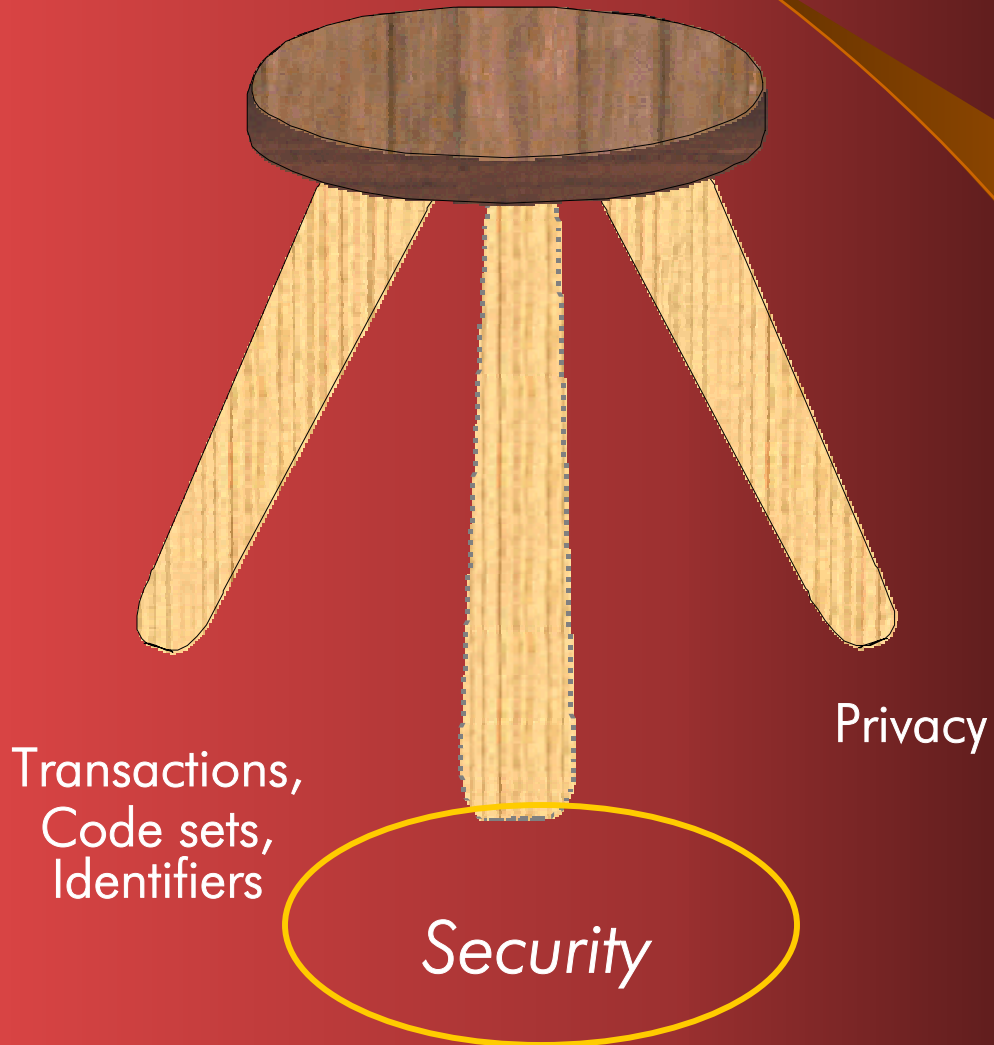
# Easy Access to the Privacy Guide MHCC Web-Site





# HIPAA

## Security “Proposed”





# HIPAA Security Standards

## An Overview

### Four Security Categories:

- Administrative Procedures

Development and implementation of security measures to protect data, and the conduct of personnel in relations to the protection of data

- Physical Safeguards

The protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as intrusion



# HIPAA Security Standards

## An Overview (Continued)

- Technical Security Services

The process that's put into place to protect information and to control and monitor individual access to information

- Technical Security Mechanisms

The process that's put into place to guard against unauthorized access to data that is transmitted over a communications network

# Security Elements - Detail

## *Administrative Procedure Activities:*

- Certification
- Chain of trust partner agreement
- Contingency plan
- Formal mechanism for processing records
- Internal audit
- Personnel security
- Security configuration management, incident procedures, and management process
- Training
- Termination procedures

# Security Elements – Detail (Continued)

## *Physical Safeguards:*

- Assigned security responsibility
- Media Controls
- Physical access controls
- Policy/guidelines on workstation use
- Secure workstation location
- Security awareness training

# Security Elements – Detail (Continued)

## *Technical Security Services:*

- Access control
- Audit control
- Authorization control
- Data authentication
- Entity authentication

# Security Elements - Detail

(Continued)

## *Technical Security Mechanisms:*

- Access control or encryption
- Alarm
- Audit trail
- Entity authentication
- Event Reporting

# Security Implementation – Small Provider Flow Chart

Preliminary Steps



On-Going Activities



On-Going Activities

**Become familiar w/ HIPAA**

**Assess actual & potential risks to your computer Systems and electronic media**

**Assess your organizations Ability to recover from any Unforeseen disaster or emergency situation**

**Determine the level of Security controls that are needed to reasonably offset your organizations security risk and exposure**

**Identify a security officer**

**Develop security policies And procedures**

**Include security awareness training in orientation & staff meetings**

**Implement physical access controls**

**Establish guidelines for removal of data**

**Implement access control measures**

**Obtain signed Chain of Trust letter**

**Use encryption software when sending PHI over the Internet**

**Activate internal software auditing capabilities**

**Self-certify the security of your computer system(s)**

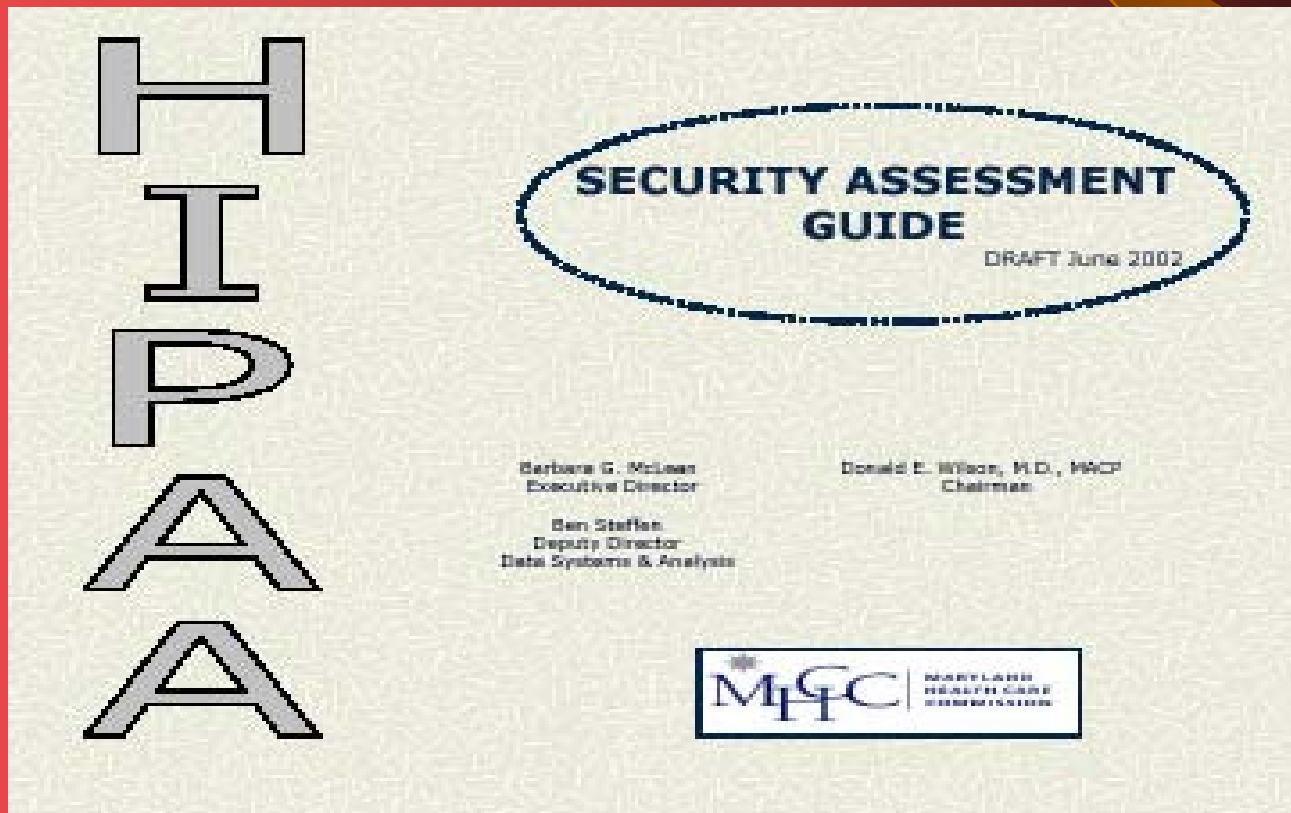
**Designate full system access to at least two employees**

**Routinely monitor your practice for compliance**

# HIPAA Assistance For Providers

- An easy to use gap assessment tool for providers:

*Available at the MHCC Web-site – October '02*





# Security Readiness Assessment Guide

- The EDI/HIPAA Workgroup decided on eight sections:
  - Introduction
  - Definitions
  - Small Provider Implementation Example
  - Assessment Guide and Work Plan
  - Administrative Procedure Checklist
  - Physical Safeguards Procedures Checklist
  - Technical Security Services Procedures Checklist
  - Technical Security Mechanisms Procedures Checklist

# HIPAA– The Change Process

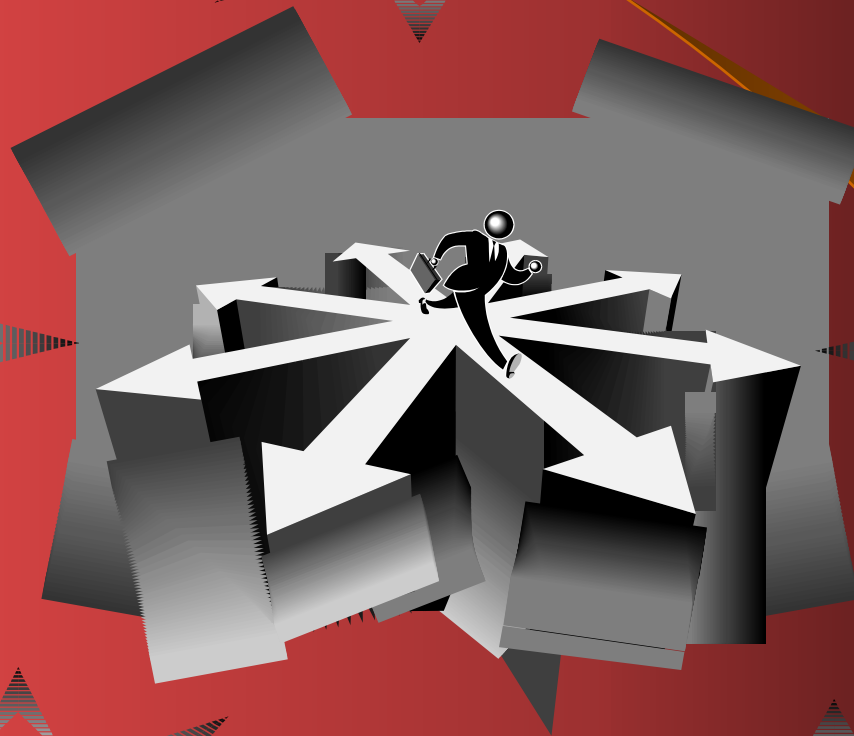
**Identify Practitioner  
Changes**

**Assessment of  
Current Knowledge:  
Skills, Organizational  
Resources and  
Change Resistance**

**Re-evaluate  
Change Process**

**Measure and  
Evaluate  
Behavioral Changes**

**Develop and  
Deliver Policies  
and Training**



# Begin Planning for HIPAA

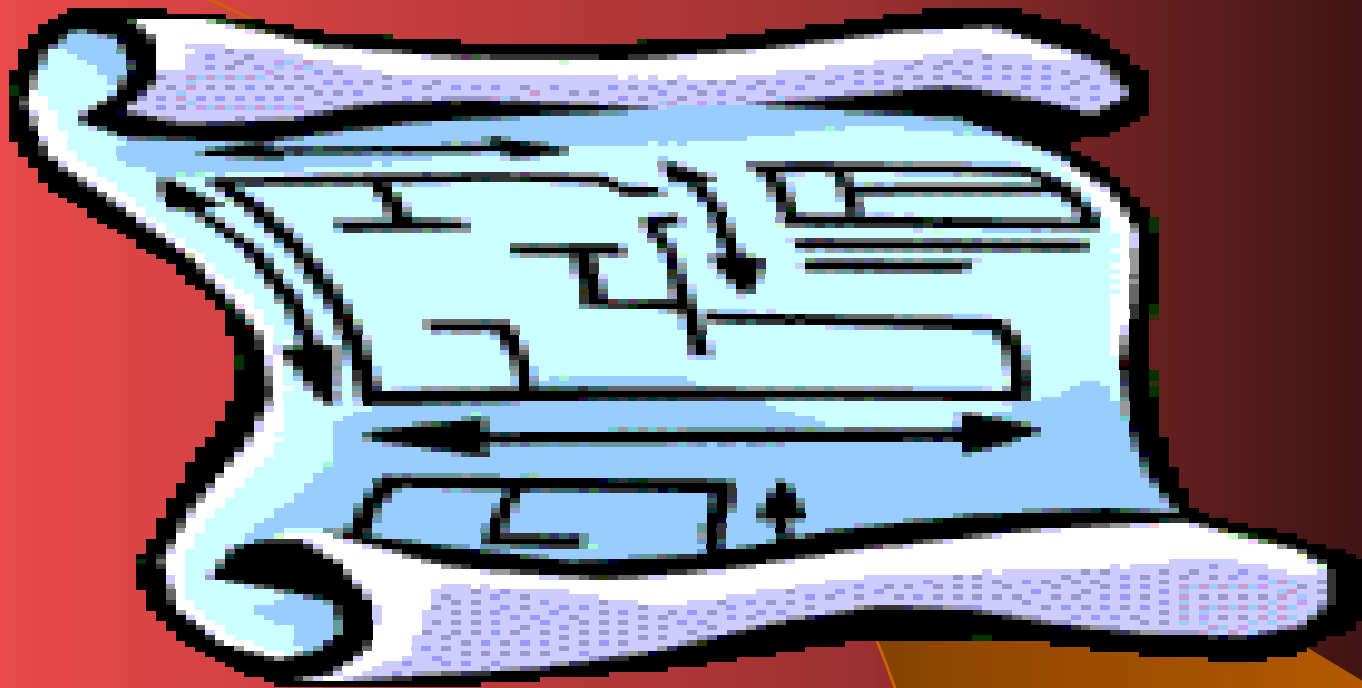


Think and educate

Conduct Assessment and Analysis

Evaluate current processes against the standards

# As You Implement HIPAA Look For Opportunities...



Use The Implementation Process To Improve  
Customer Service & Business Operations

# For More Information on HIPAA

## Official Sites

### Government sites:

<http://aspe.hhs.gov/admnsimp> - Department of Health and Human Services

<http://www.hcfa.gov/security/iseclplcy.htm> - HCFA Internet Security Policy

<http://www.wpc-wdi.com/hipaa> -- Implementation Guides

### Non-govt sites:

<http://www.wedi.org>

<http://www.nchica.org>

<http://www.hipaadvisory.com/>

### MHCC site:

<http://www.mhcc.state.md.us>



# Questions?



**Maryland Health Care Commission**